Computer Communications 34 (2011) 1708–1721

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

On performance of group key distribution techniques when applied to IPTV services

António Pinto [a,b,*], Manuel Ricardo [c]

[a] INESC Porto, Portugal
[b] Escola Superior de Tecnologia e Gestão de Felgueiras, Politécnico do Porto, Portugal
[c] INESC Porto, Faculdade de Engenharia, Universidade do Porto, Portugal

ARTICLE INFO

Article history:
Received 19 April 2010
Received in revised form 5 October 2010
Accepted 19 March 2011
Available online 3 April 2011

Keywords:
IPTV
User groups
Admission control
Multicast
Security

ABSTRACT

IPTV services consist of multiple video channels grouped in bundles, such as sports, movies or generic bundles; users typically subscribe multiple bundles, including the generic bundle. Secure IP multicast can be used to implement IPTV services, but it still has problems to be addressed. Current solutions require high computational power in video channel zapping situations, lack support for groups sourced at the users, and present a weak support for admission control in IP multicast for both sources and receivers in dynamically configured environments.

This work proposes a new, secure and efficient IPTV solution that, cumulatively: (a) enforces individual access control to groups of real-time IPTV video channels; (b) enforces IP multicast admission control for both multicast senders and receivers; (c) supports user generated videos; (d) generates low signaling overheads; (e) does not introduce perceivable delays, particularly in video channel zapping situations. Moreover, this solution can be easily integrated in the IPTV architectures being developed by ETSI and ITU-T.

1. Introduction

Current efforts to standardize video streaming over IP include functionalities required at network, transport, and session layers. The IETF multimedia architecture has defined, in particular, the RTP which enables the transmission of video, voice and multimedia contents in IP packets, along with other protocols for controlling the video streaming. More recently [1,2], these protocols have been re-used by organizations such as the ITU-T and ETSI to integrate IPTV services in the NGN architecture, defined by TISPAN. Key issues of these ETSI and ITU-T activities are the mobile-fixed service convergence, and the optimized transmission of video streams over heterogeneous access networks, namely xDSL, WiMAX and UMTS.

IP multicast is of particular appeal for IPTV services, since it enables significant savings in terms of network resources by only transmitting once for all active receivers. Despite of the scalability obtained by using multicast techniques, network operators have been reluctant to use them [14] due to their lack of native control over groups, making it difficult for network operators and service providers to perform access control, traffic accounting, and network management. Thus, the use of multicast in current IPTV services exists but it is limited, namely by not allowing user generated multicast traffic and by only allowing downlink multicast traffic on separated (virtual) circuits which are specifically used by the IPTV service.

Secure IP multicast [3–5] may be used to support the secure transmission of IP packets to groups of receivers in IPTV services but neglects access control and network management. Key distribution solutions for secure group communications usually apply key refreshing techniques upon a group change (member join or leave) in order to impose both perfect forward and backward secrecy.

On the other hand, the increasing bandwidth being offered to residential users, combined with the proliferation of techniques to produce rich user generated content, suggests that users will be compelled to generate and distribute their own real-time videos to groups of other users, directly from their premises. This scenario requires network operators to protect also user generated videos in what concerns confidentiality and access control.

The main objectives of this work are then to define a secure IPTV solution that, cumulatively: (a) enforces individual access control to groups of real-time IPTV video channels; (b) enforces IP multicast admission control for both multicast senders and receivers; (c) supports user generated videos; (d) generates low signaling overheads; (e) does not introduce perceivable delays, particularly in video channel zapping situations.

The reference scenario adopted for this work is shown in Fig. 1. It describes an IPTV service where video channels are distributed as IP packets and transmitted to a multicast address – one multi-

* Corresponding author. Tel.: +351 255314002.
E-mail addresses: apinto@inescporto.pt, apinto@inescporto.pt (A. Pinto), mricardo@inescporto.pt (M. Ricardo).

0140-3664/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2011.03.011

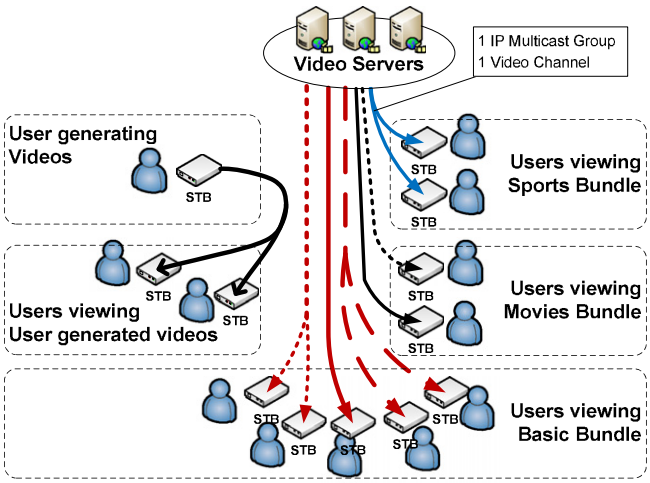

Fig. 1. Reference scenario.

cast group per video channel. Multiple video channels are grouped together, in bundles, and may be distributed to a group of receivers with equal access to the video channels of the bundle. A bundle is thus composed by several video channels, each video channel transmitted to a different multicast address. In what concerns security, common IPTV services use one key for each video channel. In this work we extend our previous secure multicast technique [3] by adding the support for multicast admission control and user generated groups. The video channels are generated by Video Servers (VS) to groups of Set-Top Boxes (STB). A STB may also generate video contents and uses heterogeneous access networks to access the IPTV service, including xDSL, WiMAX or UMTS.

This paper is organized as follows. Section 2 provides an overview of the different existing proposals for multicast admission control and summarizes their key differences. Section 3 provides an overview of secure multicast, classifying existing solutions according to four types of key distribution. Section 4 describes the key components and interfaces of the proposed solution and assesses the deployment of the proposed solution over heterogeneous access networks. Section 6 presents the obtained results. Section 7 draws the conclusions of this work.

2. Multicast admission control

Work related to IP multicast AAA is being carried out within the IETF MBONE Workgroup. In [22] the requirements for multicast AAA were specified, and in [23] a general multicast AAA framework is being designed to satisfy these requirements. Research proposals regarding AAA in IP multicast typically follow one of two approaches: the introduction of an additional control layer, or the modification of IGMP/MLD signaling. The first approach consists in introducing an intermediate control layer between IP and IGMP/MLD processing. The second approach requires the modification of the group management protocols (IGMP/MLD) in order to carry user authentication information.

2.1. Adopted notation

Table 1 presents the adopted notation. Capital letters such as A, B, C and D represent communication nodes. K_{ab} represents a symmetric key previously shared between the nodes A and B. N_a represents a nonce generated by node A. $H(M)$ represents the output of an hash function of input data M ·$\{M\}_K$ represents an M message encrypted with the key K· SEK_i represents the current Session Encryption Key (SEK) of communicating node A. $X \cdot Y$ represents field X concatenated with field Y. *APriK* represents the private key of entity A. *APubK* represents the public key of entity A. *Ts* represents a time stamp.

Table 1
Adopted notation.

A, B, C, D	Communicating nodes
K_{ab}	Symmetric pre-shared key between communicating nodes
N_a	Nonce generated by A
$H(M)$	Hash function of M
$\{M\}_K$	M encrypted with key K
SEK_i	Current session encryption key of entity A
$X \cdot Y$	Field X concatenated with field Y
APriK	Private key of entity A
APubK	Public key of entity A
Ts	Time stamp

2.2. Additional control layer approach

In [21], the authors propose a new communication protocol, the MCOP, used to exchange messages between the edge router and the MCA. The MCA is responsible for multicast session access validation and it uses IP addresses contained in the IP/IGMP packets. No protocol modifications, such as IGMP modifications, are required.

Table 2 details the message exchange for a receiver access control operation. A host wiling to participate in a group, sends an IGMP join message to access the requested group. The designated router, triggered by the join request, sends an authorization request to the MCA. Upon a successful validation by the MCA, the router will process the join request and extend the distribution tree.

In [24] the authors suggest a portal-based system where a user, in order to receive a multicast stream, would authenticate himself on a web portal and then, after a successful authentication, an entity called NetWrapper would configure the edge device to enable multicast distribution. No mention is made on how IGMP messages fit in their scheme or how would the portal retrieve information regarding the edge device associated with the request.

2.3. Protocol modification approach

SMKD [15] consists in a secure version of CBT that uses cryptographic techniques to protect the addition of routers to the distribution path, in order to impose receiver access control, and to perform group key distribution. In SMKD, each group has a GKDC that holds the group ACL and distributes cryptographic keys to authorized routers and hosts. Table 3 details the message exchange for a receiver access control operation.

A host willing to participate in a group sends an IGMP join message, modified to include a digital signed token, to its designated router. The token contains the host identification, a time stamp and a nonce. In turn, the router verifies the token and initiates the group distribution tree extension by forwarding the hosts token to the GKDC. Upon successful verification, the GKDC sends back a signed ACL and the group related cryptographic keys. At this

Table 2
MCOP protocol for receiver access control.

Sequence	Entities	Messages
1	*Host* → *Router*	IGMP/MLD Join
2	*Router* → *MCA*	Validate:Group_Address.Host_Address
3	*MCA* → *Router*	Result:Group_Address.Host_Address